CERT

Recent Federal Policies Affecting the Cybersecurity and Resiliency Landscape

Dr. Nader Mehravari, MBCP, MBCI

CERT Resilience Management Team
Software Engineering Institute
Carnegie Mellon University
http://www.cert.org/resilience/

January 23, 2014

		Form Approved OMB No. 0704-0188

Report Documentation Page

Form Approved
OMB No. 0704-0188

Public reporting burden for the collection of information is estimated to average 1 hour per response, including the time for reviewing instructions, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden, to Washington Headquarters Services, Directorate for Information Operations and Reports, 1215 Jefferson Davis Highway, Suite 1204, Arlington VA 22202-4302. Respondents should be aware that notwithstanding any other provision of law, no person shall be subject to a penalty for failing to comply with a collection of information if it does not display a currently valid OMB control number.

1. REPORT DATE **23 JAN 2014**	2. REPORT TYPE **N/A**	3. DATES COVERED

4. TITLE AND SUBTITLE **Recent Federal Policies Affecting the Cybersecurity and Resiliency Landscape**	5a. CONTRACT NUMBER
	5b. GRANT NUMBER
	5c. PROGRAM ELEMENT NUMBER
6. AUTHOR(S) **Mehravari /Nader**	5d. PROJECT NUMBER
	5e. TASK NUMBER
	5f. WORK UNIT NUMBER
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) **Carnegie Mellon Software Engineering Institute, 4500 Fifth Ave, Pittsburgh, PA 15213**	8. PERFORMING ORGANIZATION REPORT NUMBER
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)	10. SPONSOR/MONITOR'S ACRONYM(S)
	11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION/AVAILABILITY STATEMENT
Approved for public release, distribution unlimited.

13. SUPPLEMENTARY NOTES

14. ABSTRACT

15. SUBJECT TERMS

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT **SAR**	18. NUMBER OF PAGES **54**	19a. NAME OF RESPONSIBLE PERSON
a. REPORT **unclassified**	b. ABSTRACT **unclassified**	c. THIS PAGE **unclassified**			

Standard Form 298 (Rev. 8-98)
Prescribed by ANSI Std Z39-18

Notices

Outline

Setting the Stage

— What policy developments took place in February 2013?
— Why are these developments important?

Some Historical Background Relevant to Cybersecurity & Resilience

— Source of Federal Regulations
— Existing Federal Regulations
— Congressional Activities
— Presidential Executive Orders
— Presidential Policy Directive

Description of the February 2013 Developments

— Executive Order No. 13636
— Presidential Policy Directive (PPD) 21
— NIST Initiating Development of a Cybersecurity Framework

Closing Thoughts

Setting the Stage

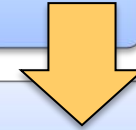- What policy developments took place in February 2013?
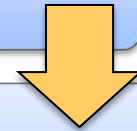- Why are these developments important?

Developments During the Week of Feb. 12, 2013

President's State of the Union Address

Executive Order

(Improving Critical Infrastructure Cybersecurity)

Presidential Policy Directive – PPD 21

(Critical Infrastructure Security and Resilience)

NIST's Plans for Developing a Cybersecurity Framework

Why are these developments important?

"...85 percent of our nation's critical infrastructure is controlled not by government but by the private sector..."

—The 9/11 Commission Report

Software Engineering Institute | Carnegie Mellon University

Critical Infrastructure

"… Systems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters …"

—Title 42, Code of Laws of the United States of America

Why are these developments important?

"… the ability to prepare for and adapt to changing conditions and withstand and recover rapidly from disruptions. Resilience includes the ability to withstand and recover from deliberate attacks, accidents, or naturally occurring threats or incidents…"

—Presidential Policy Directive – PPD 21
(February 12, 2013)

Critical Infrastructure Sectors

- Chemical
- Commercial Facilities
- Communications
- Critical Manufacturing
- Dams
- Defense Industrial Base
- Emergency Services
- Energy
- Financial Services
- Food and Agriculture
- Government Facilities
- Health Care and Public Health
- Information Technology
- Nuclear Reactors, Materials, and Waste
- Transportation Systems
- Water and Wastewater Systems
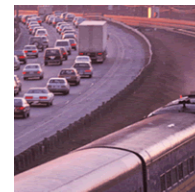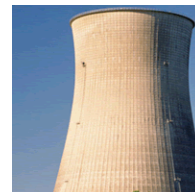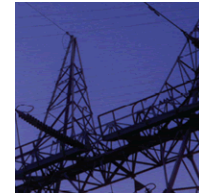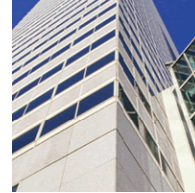
Kinetic Disruptions to Critical Infrastructure

Cybersecurity Disruptions to Critical Infrastructure

Why are these developments important?

In the past, there have been executive orders, presidential policy directives, and legislative actions with major effects on

- disaster planning
- crisis management
- identity management
- emergency communications
- critical infrastructure protection
- application of DR/BC/InfoSec national & international standards

Conditions are ripe for recent policy developments to significantly affect cybersecurity and resiliency landscapes.

Historical Background

- Source of Federal Regulations
- Existing Federal Regulations
- Congressional Activities
- Presidential Executive Orders
- Presidential Policy Directive

Sources of Federal Regulations

In the United States, cybersecurity and resiliency **regulation** comprises

Legislation
from Congress

Directives
from the Executive Branch

Existing Federal Regulations

There are few cybersecurity and resiliency regulations.

The ones that exist focus on specific industries.

The three main existing cybersecurity regulations are

1996 Health Insurance Portability and Accountability Act	Health Care Organizations
1999 Gramm–Leach–Bliley Act	Financial Institutions
2002 Homeland Security Act, which included the Federal Information Security Management Act (FISMA)	Federal Agencies

Congressional Cybersecurity Activities

Congress has been holding hearings related to cybersecurity every year since 2001.

Most recently:

Number of bills and resolutions introduced with provisions related to cybersecurity	
111th Congress *(January 2009 – January 2011)*	60+
112th Congress *(January 2011 – January 2013)*	40+
113th Congress *(as of May 22, 2013)*	17

Cybersecurity Legislation

The Obama Administration sent Congress a package of legislative proposals in May 2011

- to give the federal government new authority to ensure that corporations that own the assets most critical to the nation's security and economic prosperity are adequately addressing the risks posed by cybersecurity threats.

No comprehensive cybersecurity legislation has been enacted since 2002.

What Are Presidential Executive Orders?

U.S. presidents issue **executive orders** to help officers and agencies of the executive branch manage the operations within the federal government.

Executive Orders, by 4-Year Administration
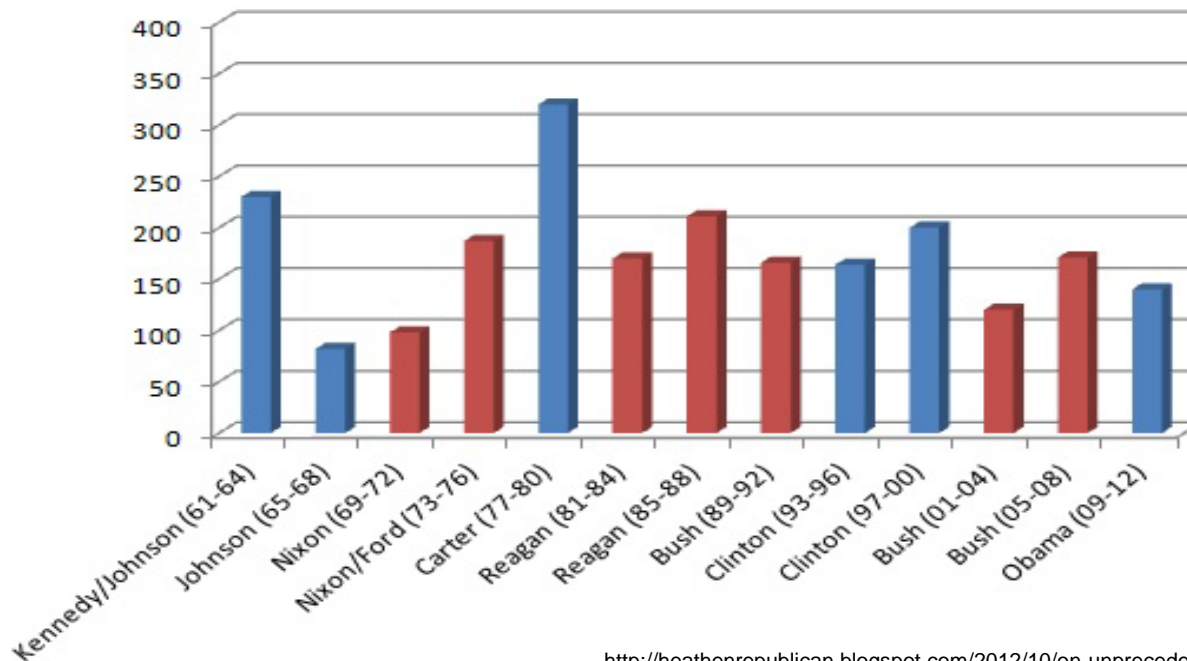
What Are Presidential Executive Orders?

Executive orders have the full force of law.

Typically made in pursuance of certain acts of Congress, some of which specifically delegate to the president some degree of discretionary power

Or are believed to take authority from power granted directly to the executive by the Constitution

What Are Presidential Directives?

A form of an executive order issued by the president of the United States

- with the advice and consent of the National Security Council

Articulate the executive's national security policy.

They carry the full force and effect of law.

Since many presidential directives pertain to the national security of the United States, many are classified.

Presidential Memorandum, August 21, 1963

President Kennedy established the **National Communications System (NCS)**

After the Cuban missile crisis

The NCS mandate included linking, improving, and extending the communications facilities and components of various federal agencies, focusing on interconnectivity and survivability.

E.O. 12472 - April 3, 1984

Assignment of National Security and Emergency Preparedness Telecommunications Functions

Superseded President Kennedy's original 1963 memorandum

Broadened the NCS

PPD-63 - May 22, 1998

Critical Infrastructure Protection

Set national goal:

- The ability to protect the nation's critical infrastructure from intentional attacks

- Any interruptions in the ability of these infrastructures to provide their goods and services must be "brief, infrequent, manageable, geographically isolated, and minimally detrimental to the welfare of the United States."

Homeland Security Act of 2002

Was introduced in the aftermath of

- September 11 attacks
- mailings of anthrax spores

Established the

- **Department of Homeland Security (DHS)**
- **cabinet-level position of secretary of homeland security**
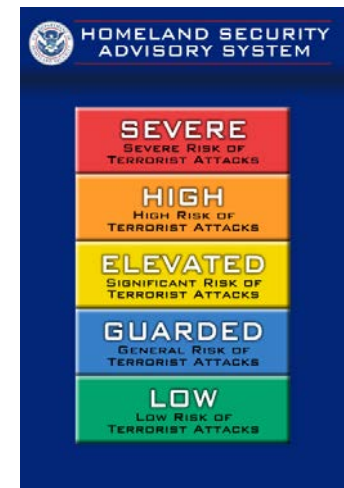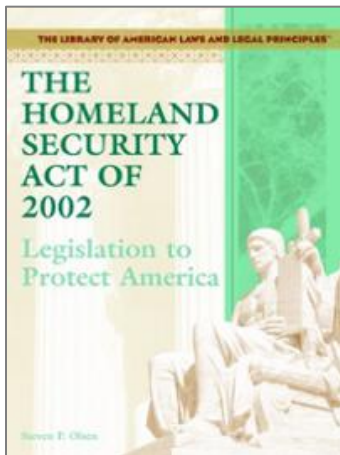
HSPD-7 – December 7, 2003

Critical Infrastructure Identification, Prioritization, and Protection

Replaced PPD-63

Aimed to unify protection efforts for critical infrastructure and key resources (CIKRs) across the country

Focus of HSPD-7
Terrorist attacks
Physical systems

National Infrastructure Protection Plan

Partnering to enhance protection and resiliency

2009
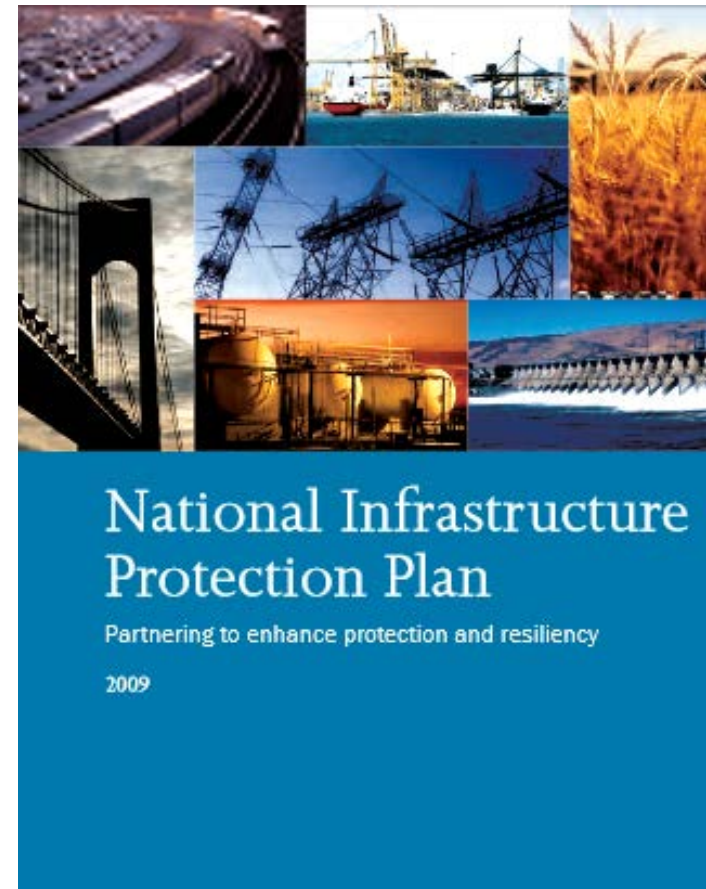
E.O. 13407 - June 26, 2006

Public Alert and Warning System

[Following](#) Hurricane Katrina

Ordered DHS to establish a new program to integrate and modernize the nation's existing population warning systems, such as

- Emergency Alert System (EAS)
- National Warning System (NAWAS)
- Commercial Mobile Alert System (CMAS)
- NOAA Weather Radio All Hazards

Subsequently termed the Integrated Public Alert and Warning System (IPAWS)

Description of February 2013 Policy Developments

- Executive Order No. 13636
- Presidential Policy Directive (PPD) 21
- NIST Initiated Development of a Cybersecurity Framework

Executive Order

Executive Order No.

- 13636

Issuance Date

- Tuesday, February 12, 2013

Title

- Improving Critical Infrastructure Cybersecurity

Overall Objective

- **To enhance the security and resilience of the nation's critical infrastructure**

Classification

- Unclassified

Presidential Policy Directive

Presidential Policy Directive No.

- PPD-21

Issuance Date

- Tuesday, February 12, 2013

Title

- **Critical Infrastructure Security and Resilience**

Classification

- Unclassified

Messages of Executive Order & PPD

"…Our country's reliance on cyber systems to run everything from power plants to pipelines and hospitals to highways has increased dramatically, and our infrastructure is more physically and digitally interconnected than ever…"

"…The cyber threat to critical infrastructure continues to grow and represents one of the most serious national security challenges we must confront…"

"…Steps must be taken to enhance existing efforts to increase the protection and resilience of critical infrastructure, while maintaining a cyber environment that encourages efficiency, innovation, and economic prosperity, while protecting privacy and civil liberties…"

Overall Objectives of EO and PPD

To strengthen the security and resilience of critical infrastructure against evolving threats through an updated and overarching national framework that acknowledges the increased role of cybersecurity in securing physical assets.

Together, the EO and PPD create an opportunity to reinforce the need for holistic thinking about security risk management and drive action toward a whole of community approach to security and resilience.

Sections of the Executive Order

- Policy

- Critical Infrastructure

- Policy Coordination

- Cybersecurity Information Sharing

- Privacy and Civil Liberties

- Consultative Process

- Baseline Framework

- Voluntary Critical

- Identification of C

- Adoption of Framework

It is the policy of the United States to enhance the security and resilience of the nation's critical infrastructure and to maintain a cyber environment that encourages efficiency, innovation, and economic prosperity while promoting safety, security, business confidentiality, privacy, and civil liberties.

Sections of the Executive Order

- Policy

- Critical Infrastructure

- Policy Coordination

- Cybersecurity Information Sharing

- Privacy and Civil Liberties Protections

- Consultative Process

- Baseline Framework to Reduce Risk ~~to~~ ~~Infrastructure~~

- Voluntary Critical Infrastructure

- Identification of Critical Infrastructure

- Adoption of Framework

DHS to establish a new information sharing program to provide both classified and unclassified threat and attack information to U.S. companies

Software Engineering Institute | Carnegie Mellon University

Sections of the Executive Order

- Policy

- Critical Infrastructure

- Policy Coordination

- Cybersecurity Information Sharing

- Privacy and Civil Liberties Protections

- Consultative Process

- Baseline Framework to Reduce Risk to Critical Infrastructure

- Voluntary Critical Infrastructure Cyb

- Identification of Critical Infrastructur

- Adoption of Framework

Agencies are required to incorporate privacy and civil liberties safeguards in their cybersecurity activities.

Sections of the Executive Order

- Policy

- Critical Infrastructure

- Policy Coordination

- Cybersecurity Information Sharing

- Privacy and Civil Liberties Protections

- Consultative Process

- Baseline Framework to Reduce Risk to Critical Infrastructure

- Voluntary Critical Infrastructure Cybersecurity Program

- Identification of Critical Infrastructure at Greatest Risk

- Adoption of Framework

NIST to lead the development of a Cybersecurity Framework to reduce risk to critical infrastructure

Sections of Presidential Policy Directive

Introduction

Policy

Roles and Responsibilities

Three Strategic Imperatives

Innovation and Research a

Implementation of the Dire

Designated Critical Infrastr
and Sector-Specific Agenc

Definitions

Critical infrastructure must be secure and able to withstand and rapidly recover from all hazards.

This directive establishes national policy on critical infrastructure security and resilience.

Sections of Presidential Policy Directive

Introduction

Policy

Roles and Responsibilities

Three Strategic Imperatives

Innovation and Research and Development

Implementation of the Directive

Designated Critical Infrastructure and Sector-Specific Agencies

Definitions

Address the security and resilience of critical infrastructure in an integrated, holistic manner to reflect this infrastructure's interconnectedness and interdependency.

CERT | Software Engineering Institute | Carnegie Mellon University

Sections of Presidential Policy Directive

Introduction

Policy

Roles and Responsibilities

Three Strategic Imperatives

Innovation and Research and Development

Implementation of the Directive

Designated Critical Infrastructure Sectors
and Sector-Specific Agencies

Definitions

Calls for a comprehensive R&D plan for critical infrastructure to guide the government's effort to enhance and encourage market-based innovation

Sections of Presidential

Introduction

Policy

Roles and Responsibilities

Three Strategic Imperatives

Innovation and Research

Implementation of the Directive

Designated Critical Infrastructure Sectors
and Sector-Specific Agencies

Definitions

1. *Chemical*
2. *Commercial Facilities*
3. *Communications*
4. *Critical Manufacturing*
5. *Dams*
6. *Defense Industrial Base*
7. *Emergency Services*
8. *Energy*
9. *Financial Services*
10. *Food and Agriculture*
11. *Government Facilities*
12. *Health Care and Public Health*
13. *Information Technology*
14. *Nuclear Reactors, Materials, & Waste*
15. *Transportation Systems*
16. *Water and Wastewater Systems*

Policy Directive

RESILIENCE ... the ability to prepare for and adapt to changing conditions and withstand and recover rapidly from disruptions. Resilience includes the ability to withstand and recover from deliberate attacks, accidents, or naturally occurring threats or incidents.

Three ___ gic Imperatives

Innov___ and Research and Development

Imple___ tation of the Directive

Desig___ ated Critical Infrastructure and S___ ector-Specific Agen___

ALL HAZARDS ... natural disasters, cyber incidents, industrial accidents, pandemics, acts of terrorism, sabotage, and destructive criminal activity targeting critical infrastructure.

Definitions

PPD-21 Replaces HSPD-7 of 2003

To account for

- new risk environment
- key lessons learned
- drive toward enhanced capabilities

HSPD-7
Terrorist attacks
Physical systems

PPD-21
Security & resilience of CI (protection + operating under stress)
All hazards
Recognizes that CI cybersecurity is a matter of national security
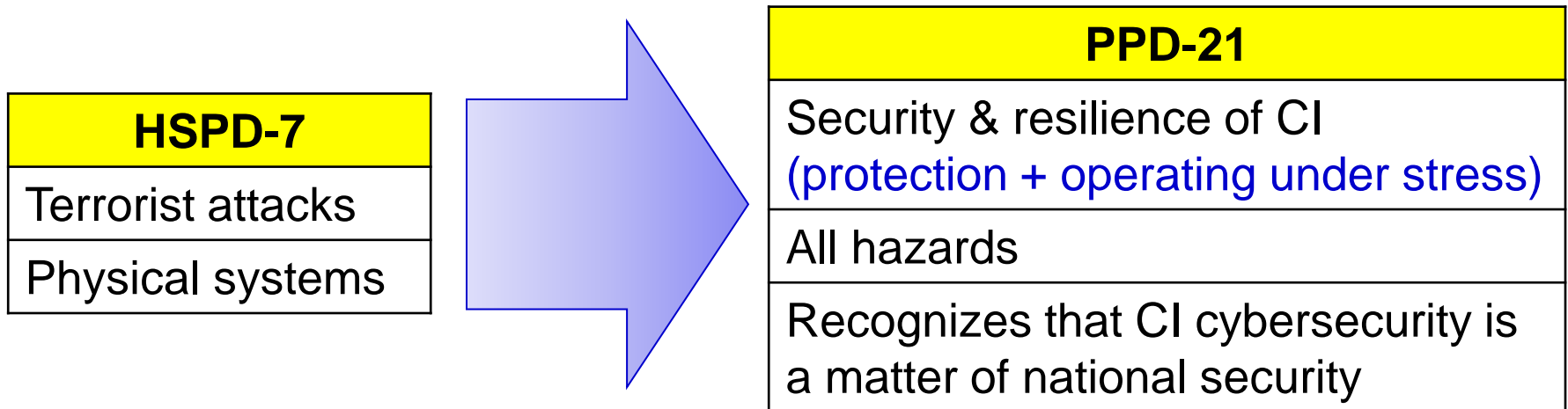
Aspects of OE/PPD Related to Framework

NIST shall

- develop a cybersecurity framework (CSF)

DHS shall

- establish a voluntary program to promote the adoption of the CSF

Regulatory agencies shall

- review the framework and determine if current regulations are sufficient
- develop new regulations if current ones are insufficient

NIST Framework Development Process

Engage the Framework Stakeholders

Collect, Categorize, & Post RFI Responses

Analyze RFI Responses

Select Framework Components

Prepare & Publish Preliminary Framework

Release Official Framework

- February 2013 – NIST Issues RFI

- April 3, 2013 – 1st Framework Workshop

- April 8, 2013 – Post RFI Responses

- May 15, 2013 – Identify Common Practices/Themes

- May 29-31, 2013 – 2nd Framework Workshop

- June 2013 – Draft Initial Framework

- July 2013 – 3rd Framework Workshop

- September 2013 – 4th Framework Workshop

- October 2013 – Publish Preliminary Framework

- November 2013 – 5th Framework Workshop

- December 2013 – Public Comment Period

- February 2014 – Release Official Framework

Closing Thoughts

Observation:

Taking actions "before" & "after" major national disruptive events

- After Cuban Missile Crisis
  - Presidential Memorandum of August 21, 1963 (NCS)
- After September 11
  - HSPD 1, 5, 7, 8, 12, 20, 21
  - Homeland Security Act of 2002
  - PS-PREP
- After Mailings of Anthrax Spores
    Homeland Security Act of 2002 (DHS)
- After Hurricane Katrina
  - EO-13407 (IPAWS)

- PPD-63 (CIP)
- EO-13636 and PPD-21 (CI Security and Resilience)

Observation:

PPD-21 accounts for

- new risk environment
- key lessons learned
- drive toward enhanced capabilities

HSPD-7
Terrorist attacks
Physical systems

→

PPD-21
Security & resilience of CI (protection + operating under stress)
All hazards
Recognizes that CI cybersecurity is a matter of national security
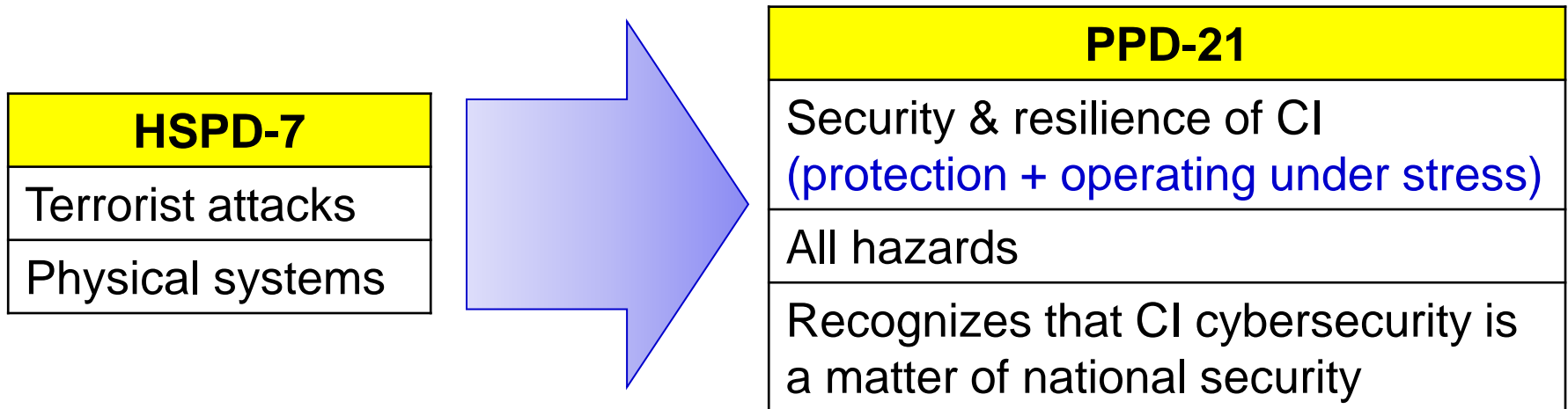
Observation (& Question to Be Considered)

Policies and doctrines around kinetic attacks on U.S. interests are mature, but they fail to provide needed clarity when applied to cyber-based attacks, especially those of foreign state actors.

For example…

Question: Enable Active Defenses?

An active shooter in a bank lobby would likely meet deadly force in response.

Should organizations be legally allowed to fight back when under cyber attack?

Do we need policies and regulations governing such active cyber defenses?

July 12, 2013

THE WALL STREET JOURNAL.

U.S. EDITION ▾   Friday, July 12, 2013 As of 12:57 AM EDT

Home | **World** ▾ | U.S. ▾ | New York ▾ | Business ▾ | Tech ▾ | Markets ▾ | Market Data | Opinion ▾ | Life & Culture ▾ | Real Esta

ASIA NEWS | Updated July 12, 2013, 12:57 a.m. ET

U.S., Firms Draw a Bead on Chinese Cyberspies

By DANNY YADRON and SIOBHAN GORMAN

The U.S. government gave American Internet providers addresses linked to suspected Chinese hackers earlier this year as part of a previously undisclosed effort aimed at blocking cyberspying, current and former U.S. officials said.

The push reflects a significant shift in levels of cooperation between the government and Internet companies amid rising concerns over hacking. It

The efforts represent a rare glimpse into what NSA Director Gen. Keith Alexander and other officials call "active defense," which they characterize as exercising self-defense in cyberspace. How such activities are executed remains largely cloaked in mystery.

Question: National Defenses

If a foreign state fired a missile at a U.S. bank HQ, it would meet immediate military defense.

Should military-grade cyber defenses be deployed to protect U.S. businesses that are under attack by foreign states?

Do we need another exception to the Posse Comitatus Act to enable military cyber response to large-scale cyber attacks on U.S. critical infrastructure?

Role of Federal Government?

THE WALL STREET JOURNAL.

Nader's Journal ▼

U.S. EDITION ▼   Sunday, May 12, 2013 As of 4:03 PM EDT

Home | World ▼ | U.S. ▼ | New York ▼ | Business ▼ | Tech ▼ | Markets ▼ | Market Data | Opinion ▼ | Life & Culture ▼ | Real Estate ▼ | Management ▼ | C-Su

JOURNAL REPORTS | Updated May 10, 2013, 4:32 p.m. ET

Should Companies Be Required to Meet Certain Minimum Cybersecurity Protections?

By SIOBHAN GORMAN

U.S. companies appear to have lots of not-so-secret secrets.

Intelligence reports, for instance, say China and Russia have been pilfering vast quantities of secrets from U.S. companies, while U.S. officials say Iranian-backed hackers have mounted a relentless campaign against U.S. banks.

President Barack Obama in February

Role of Federal Government?

THE WALL STREET JOURNAL.

U.S. EDITION ▾ Friday, June 14, 2013 As of 7:51 PM EDT

Home | World ▾ | U.S. ▾ | New York ▾ | Business ▾ | Tech ▾ | Markets ▾ | Market Data | Opinion ▾

MARKETS | June 14, 2013, 7:51 p.m. ET

A Call to Arms for Banks

Regulators Intensify Push for Firms to Better Protect Against Cyberattacks

Article | Video | Stock Quotes | Comments (12)

✉ Email | 🖨 Print | ➕ Save ▾ | f | 🐦 | g+ | in | A A

By MICHAEL R. CRITTENDEN

WASHINGTON—U.S. regulators are stepping up calls for banks to better-arm themselves against the growing online threat hackers and criminal organizations pose to individual institutions and the financial system as a whole.

The push comes as government officials grow increasingly concerned about the ability of a cyber attack to cause significant disruptions to the financial system. Banks such as J.P. Morgan Chase & Co., Bank of America Corp. [BAC +0.73%] and Capital One Financial Corp. [COF +0.70%] have been targeted by cyber assaults in recent years, including potent "denial-of-service" strikes that took down some bank websites of dollars

Software Engineering Institute | Carnegie Mellon University

Thank you for your attention…

References

Specific to the Executive Order

- http://www.whitehouse.gov/the-press-office/2013/02/12/executive-order-improving-critical-infrastructure-cybersecurity
- http://www.whitehouse.gov/the-press-office/2013/02/12/executive-order-improving-critical-infrastructure-cybersecurity-0
- http://www.dhs.gov/news/2013/02/13/fact-sheet-executive-order-cybersecurity-presidential-policy-directive-critical
- https://www.federalregister.gov/articles/2013/02/19/2013-03915/improving-critical-infrastructure-cybersecurity

Specific to PPD-21

- http://www.whitehouse.gov/the-press-office/2013/02/12/presidential-policy-directive-critical-infrastructure-security-and-resil
- http://www.whitehouse.gov/the-press-office/2013/02/12/fact-sheet-presidential-policy-directive-critical-infrastructure-securit
- http://www.hsdl.org/?abstract&did=731087
- http://www.dhs.gov/news/2013/02/13/fact-sheet-executive-order-cybersecurity-presidential-policy-directive-critical

Specific to NIST Framework

- http://www.commerce.gov/news/press-releases/2013/02/13/national-institute-standards-and-technology-initiates-development-new
- http://www.nist.gov/itl/upload/rfi_02_12_13.pdf
- https://www.federalregister.gov/articles/2013/02/26/2013-04413/developing-a-framework-to-improve-critical-infrastructure-cybersecurity#h-4
- http://www.nist.gov/itl/cyberframework.cfm
- http://www.nist.gov/itl/csd/framework-022613.cfm

Other References

- Rita Tehan, "Cybersecurity: Authoritative Reports and Resources," Congressional Research Service, January 17, 2013. http://www.fas.org/sgp/crs/misc/R42507.pdf
- Franklin Reeder, et.al., "Updating U.S. Federal Cybersecurity Policy and Guidance," Center for Strategic & International Studies, October 2012.
- Eric A. Fischer, "Federal Laws Relating to Cybersecurity: Discussion of Proposed Revisions," Congressional Research Service, November 9, 2012. (http://www.fas.org/sgp/crs/natsec/R42114.pdf)
- http://en.wikipedia.org/wiki/Executive_order
- http://en.wikipedia.org/wiki/Presidential_directives